Sociedad de la información y marketing

Colin, Caroline; Poullet, Yves

Published in:
Protección de datos personales en la sociedad de la información y la vigilancia

Publication date:
2011

Document Version
le PDF de l'éditeur

CAPÍTULO IX

SOCIEDAD DE LA INFORMACIÓN Y MARKETING: *CASE STUDY*(*)

Caroline COLIN

Doctora en Derecho e Investigadora del Centre de Recherche Informatique et Droit (CRID), Universidad de Namur

Yves POULLET

Profesor de las Facultades de Derecho de Namur y de Liège, Rector de la Universidad de Namur

(*) Esta contribución se inscribe en el marco de la investigación realizada por el CRID en el marco del proyecto MIAUCE, proyecto del 6.º Programa Marco de la Unión Europea que analiza ciertas tecnologías multimodales de vigilancia (*Multi modal Analysis and Exploration of Users within a controlled Environment*, IST Call 5, FP6-2005-IST-5). Los autores agradecen la colaboración de los investigadores del CRID que trabajan en el proyecto, en particular Antoinette ROUVROY, Doctora en Derecho e investigadora calificada FNRS, y Denis DARQUENNES, informático y físico. A la vez, este proyecto agrupa un vasto consorcio de centros de investigación universitarios que desarrollan tecnologías de observación multimodales del comportamiento humano (en particular el reconocimiento de emociones y de desplazamientos) y de equipos de investigación en materia ética, jurídica y sociológica por un lado y, por otro, de empresas interesadas en el desarrollo de aplicaciones nacidas de estas tecnologías. Sobre este programa, véase el sitio del proyecto MIAUCE (http://www.miauce.org).
Esta contribución se cerró en junio de 2009.
Traducción de María Rosa LLÁCER MATACÁS.

SUMARIO:

I. INTRODUCCIÓN

§ 1. La reflexión que se propone pretende subrayar los riesgos que las nuevas aplicaciones de las tecnologías de la información y de la comunicación representan para el consumidor. Estas aplicaciones se desarrollan por laboratorios de investigación y, en algunos casos, ya se están implementando de modo todavía experimental en grandes superficies. Se basan en tecnologías de recogida de datos a distancia como el RFID, en *software* que permite prever los desplazamientos de los consumidores y, finalmente, en métodos de *profiling*. Su finalidad es, pues, adquirir un conocimiento de la clientela lo más individualizado posible, con el objeto de ofrecer al consumidor el servicio y/o la publicidad más apropiados.

Analizaremos dos tipos de cuestiones jurídicas. La primera (Capítulo 1) estudia las implicaciones que el desarrollo del estado de la cuestión puede tener en materia de protección de los datos de carácter personal y, en sentido más amplio, de las libertades y la dignidad humana. Nuestro propósito subraya la dificultad de las legislaciones actuales para responder total y adecuadamente a los riesgos incurridos por el consumidor y aboga por profundizar en ciertos conceptos y principios contenidos en las legislaciones sobre protección de los datos e, incluso, por algunas nuevas reglamentaciones. La segunda cuestión (Capítulo 2) se refiere a las legislaciones de protección de los consumidores. ¿En qué medida estas nuevas aplicaciones no podrían constituir en ciertos casos prácticas desleales e incluso discriminatorias, condenadas por nuestras legislaciones europeas de protección de los consumidores?

Al término de esta doble reflexión, el artículo apuesta, en conclusión, por una aproximación cruzada o acumulada de estos dos tipos de pro-

tección, la de los consumidores por un lado, y la de la protección de los datos por otro. Esta aproximación reúne así lo que se ha dado en llamar la «*Consumer Privacy Approach*» puesta de relieve en los Estados Unidos, cuyo interés vamos a mostrar. Por otro lado, el artículo subraya la urgente necesidad de un debate social sobre estas nuevas tecnologías que auguran una «sociedad de la observación»[1] y, en particular, sobre la necesidad de una reflexión fundamental sobre los derechos del hombre en el contexto de esta sociedad.

II. CONTEXTO DEL ESTUDIO

Conviene, ante todo, presentar el guión que servirá de base a nuestro estudio (A), antes de proceder a un extracto de los riesgos incurridos por los ciudadanos que están relacionados con estas nuevas aplicaciones (B).

1. El escenario: tarjetas de fidelidad provistas de «chip» RFID y probadores en línea

§ 2. La mejora en el trato de la clientela se realiza gracias a su *profiling*, realizado a partir de los datos almacenados en su tarjeta de fidelidad gracias a *chips* RFID[2]. Inicialmente, los comerciantes recolectan las informaciones referentes a las compras de los clientes, que pueden inscribirse o no sobre las tarjetas de fidelidad. Asimismo, la presencia del chip RFID en la tarjeta permite seguir a la persona en sus desplazamientos por las diferentes secciones, gracias a los lectores situados en el supermercado. El guión aún puede completarse. La presencia conjunta de chips RFID en la tarjeta de fidelidad, por un lado, y en los productos ofrecidos por otro, permite conocer los productos adquiridos, aquellos que solo han sido objeto de

(1) Definición dada en el *rapport* MIAUCE (citado), del «*multimodal observation paradigm*»: «*this paradigm combines multimodal capture of data "extracted" from human bodies (facial expressions, eye gaze, postures and motions) with an implicit understanding or interpretation of these data as valid and privileged sources of "truth" about the persons, their preferences, intentions etc. following the preconception according to which the "body does not lie" whereas, a contrario, anything transiting through the prism of individuals' consciousness is a priori suspect and unreliable*».

(2) Sobre los RFID y sus múltiples aplicaciones, véase Darquennes, D. y Poullet, Y., «RFID: Quelques réflexions introductives à un débat de société», *RDTI*, Janv. 2007, págs. 255 a 285.

aproximación, e incluso escogidos y luego desechados. La presencia de un producto en el carrito de la compra unido a la localización de la persona en el almacén permite, mediante un vídeo situado sobre el carrito, llamar la atención del consumidor sobre el interés en adquirir un producto que se casa perfectamente con otro: tal vino para tal queso. Todos estos datos se analizan para elaborar los perfiles de consumo. El cliente que entra en un almacén de la cadena puede ver cómo aparece automáticamente, en el vídeo situado sobre el carrito, la lista de sus compras habituales, cómo se le recuerda un determinado olvido o se le sugiere una compra en promoción o relacionada con sus gustos.

Se pone en evidencia el interés de la tarjeta si, además de los descuentos propuestos y de los consejos y servicios que el cliente recibe a lo largo de su visita del supermercado, se relacionan otras ventajas con el registro automático de la tarjeta o mediante la tarjeta. Así, algunos almacenes ya proponen el sistema de pago sin cajera. El cliente que ha llenado el carrito de artículos provistos de chips RFID ya no tiene que hacer cola en la caja: las compras se contabilizan automáticamente y el pago se realiza vinculando aquella tarjeta con su tarjeta de crédito. Cabe añadir que conservar el certificado de garantía deja de ser necesario cuando la persona puede identificarse mediante la tarjeta y acreditar la compra del producto sobre el que desea reclamar. Algunas cadenas de grandes almacenes como Wal-Mart (Norteamérica) y Metro (Alemania) ya están proponiendo estas ventajas.

§ 3. Dos variables del guión son útiles para nuestro análisis. Primero, cabe imaginar que los clientes del supermercado podrían probarse virtualmente trajes o peinados, gracias a los sitios web de estas tiendas y a la tarjeta de fidelidad que los identifican y permiten realizar los pagos en línea, digitalizando una de sus fotos, o sencillamente introduciendo sus medidas. Se puede añadir que los datos así captados a través del sitio web pueden unirse a datos almacenados en la tarjeta de fidelidad con el objeto de mejorar el perfil, en particular mediante el análisis automatizado de las reacciones psicológicas y de los gustos del consumidor.

Podemos proponer una segunda variante. Si la tarjeta permite identificar a su portador, «trazarlo» de una visita a otra y memorizar las operaciones efectuadas, podemos imaginar el funcionamiento de sistemas menos sofisticados: un chip RFID activo y pasivo se instala en el carrito del cliente que entra, estando dotado el carrito de una pantalla vídeo, como en el guión

completo. Este chip permitirá localizar al cliente X y registrar la cesta de productos que constituye; desde luego, el supermercado dispondrá de poca información pero aun así podemos imaginar un *profiling* limitado que permitirá dirigirle determinados consejos publicitarios.

§ 4. En conclusión, el guión de las nuevas aplicaciones vinculadas a las tecnologías TIC revela la complejidad de los sistemas de información que las operan. Estos sistemas permiten compilar todos los datos recogidos y, a partir de su almacenamiento, cruzarlos de forma aleatoria para obtener estadísticamente perfiles, a menudo muy precisos, de las personas cuyos datos han sido registrados e incluso de futuros clientes. Así, se detecta que a partir de un determinado recorrido en el interior del almacén, combinado con la presencia de determinados productos en la cesta de la compra, se puede deducir un interés estadísticamente confirmado por la compra de un producto determinado. Cabe observar que estas operaciones de *profiling*[3], posibles gracias a la colecta de informaciones, mezclan a la vez datos «*objetivos*», como la frecuencia de las visitas al almacén, el número y el tipo de artículos adquiridos, con datos «*subjetivos*», como la preferencia por un determinado color de traje, etc.

2. Los riesgos de la sociedad de la observación y del *profiling*

§ 5. Este escenario ilustra los riesgos que representa lo que se ha dado en llamar la sociedad de la observación[4]. Así, cabe evocar los peligros nacidos:

— del desequilibrio entre los poderes respectivos[5] de los responsables del tratamiento por un lado, que disponen de una información cada vez más y más abundante y pegada a la vida y actitudes del consumidor y, por otro, del ciudadano o consumidor afectados. Este desequilibrio

(3) Sobre las decisiones tomadas sobre la base del *profiling* de los individuos, léase Dinant, J. M.; Lazaro, C.; Poullet, Y.; Rouvroy, A., «*Rapport* al Comité consultivo "Convention n. 108" del Consejo de Europa», septiembre 2008, disponible en el sitio del Consejo de Europa. Véase igualmente, editado por Hildebrandt, M. y Gutwirth, S., *Profiling the European citizen, Cross disciplinary Perspectives*, Springer Science, Dordrecht, Países Bajos, 2008.

(4) Véase definición *supra* nota núm. 2.

(5) Solove, D. J., «Privacy and Power: Computer Data Bases and Metaphors for Information Privacy», 53 *Stanford Law Review*, 2001, 6, págs. 1393 y ss.

puede conducir a todo tipo de discriminaciones. Así, se conoce la técnica del *adaptative pricing* desarrollada por Amazon, la librería más poderosa en línea que, con arreglo al perfil de un candidato a comprador, decide el precio fijado en el sitio web. Yendo más allá, se puede pensar en la exclusión automática del acceso a ciertos servicios o productos de personas juzgadas poco interesantes a partir de su perfil;

— de la «descontextualización»[6]: las personas afectadas han «emitido» los datos que circulan por la red para un fin preciso o en un contexto particular. Los cruces de toda clase de datos, procedentes de diversas fuentes, engendran el miedo a ser juzgado «fuera de contexto»;

— de la opacidad[7] del funcionamiento, tanto de los **terminales** (las *cookies*, los RFID) como de las **infraestructuras** (véase los «agentes distribuidos», localizados a lo largo de los sistemas de información como los denominados de inteligencia ambiental). Esta opacidad conlleva el

(6) Nissenbaum, H., «Privacy as contextual Integrity», 79 *George Washington Law Rev.*, 2004, págs. 150 y ss. El autor afirma: «*the freedom from scrutiny and zones of "relative insularity" are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act and decide without giving account to others or being fearful of retribution*».

(7) *Cf.* la Sentencia constitucional en el asunto del censo (*Bundesverfassungsgerichtshof*, 15 de diciembre de 1983, *EuGRZ*, 1983, págs.171 *et* ss.). La tentación de los ciudadanos es la de adoptar el comportamiento que creen esperado por la sociedad y de no osar expresarse libremente, lo que es perjudicial para nuestras democracias: «*The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would have also impact the common good ("Gemeinwohl"), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate*».

miedo a tratamientos no solicitados, no queridos y, luego, la voluntad de conformarse a desarrollar solo los comportamientos que se perciben como los esperados en el entorno de estos nuevos lugares de vigilancia invisible;

— del **reduccionismo**[8]: los datos recogidos en ocasión de los acontecimientos incluso más insignificantes de nuestra vida (nuestra parada delante de tal sección de supermercado, nuestra indecisión al adquirir un determinado producto, la reacción delante de una determinada emisión) se multiplican cada vez más y los sistemas de información nos analizan a través estos datos y reducen nuestras personalidades, nuestra identidad, a «perfiles» creados a partir de nuestros propios datos pero, sobre todo, a partir de datos ajenos; y todo ello con arreglo a criterios y en vista a finalidades definidas por quienes utilizan estos datos, e incluso directamente por el dispositivo tecnológico[9]. En los sistemas de inteligencia ambiental el hombre, puesto en la red con un conjunto de objetos que lo rodean, se convierte en un objeto comunicante más dentro de esta red y es el acercamiento de estos «objetos» (mi presencia en la sección de quesos) lo que va a desencadenar una acción basada en mi perfil (el recordatorio de mi compra anterior y la perfecta combinación entre tal queso con el vino que acabo de adquirir);

(8) Karst ya denunció este peligro de «reduccionismo» en 1966 («The files: Legal Control Over the Accuracy and Accessibility of Stored Personal Data», 31 *Law and Contemporary problems*, 1966, pág. 361), subrayando el peligro de «*a centralized, standardized data processing* » que solo retiene como significativos, en relación con la investigación, los hechos captados y tratados por el ordenador. En el mismo sentido, véase Rosen, J., *The unwanted Gaze: the Destruction of Privacy in America*, 2000, citado por Solove, D. J., *ibidem*, pág. 424: «*Privacy protects us from being misdefined and judged out of context in aworld of short attention spans, a world in which information can easily be confused with knowledge*».

(9) Es precisamente la razón del art. 15 de la Directiva europea 95/46 en materia de protección de datos que prevé disposiciones en materia de sistemas automatizados de decisión. Tal como revelan los trabajos preparatorios: «*This provision is designed to protect interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institution deprives the individual the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his "data shadow"*».

— de la abolición de la distinción entre **esfera pública y esfera privada**[10]. El hombre perdido en la muchedumbre de unos grandes almacenes puede ser seguido, trazado; incluso en su casa, encerrado bajo doble llave, el uso del ordenador conectado a internet permite espiarlo y penetrar en sus secretos de alcoba. Regresaremos sobre este punto. Tradicionalmente y a los ojos del derecho, la protección del domicilio físico, lugar inviolable, aparecía como algo fundamental para la construcción de la personalidad del individuo. Actualmente esta noción también se halla conmocionada por el desarrollo tecnológico.

En conclusión, detectamos el riesgo que el Tribunal Constitucional alemán ya identificó en 1983[11] en el caso de los censos estadísticos, de una normalización de los comportamientos y de los pensamientos de los ciudadanos[12] impuesta por la tiranía de un poder informativo difuso, inasequible y con un poder sin límites[13].

(10) Sobre esta distinción clásica y su radical replanteamiento, Fichbaum, J. A., «Towards an autonomy-based theory of constitutional Privacy: Beyond the ideology of familial privacy», *Harvard Civil Rights – Civil Liberties Review*, 1979, 14, págs. 361-384. Sobre este punto léase igualmente, Solove, D. J., «Conceptualizing Privacy», 90 *California Law Review*, 2002, especialmente las págs. 1138 y 1139.

(11) *Bundesverfassungsgericht*, 15 de diciembre de 1983, *EuGRZ*, 1983, págs.171 y ss. Sobre esta decisión, léase Riedl, E. H., «New bearings in German Data Protection», *Human Rights Law Journal*, 1984, Vol. 5, núm. 1, págs. 67 y ss.; Burkert, H., «Le jugement du Tribunal Constitutionnel fédéral allemand sur le recensement démographique et ses conséquences», *Dr. Inf.*, 1985, págs. 8 y ss.

(12) Véase Lyon, D., «An electronic Panopticon. A sociological critique of the surveillance society», *Sociological Review*, 1993, 41(4), 653-678. Para una análisis de estos planteamientos, véase Rouvroy, A., «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Inteligence» (September 11, 2007). Disponible en SSRN: http://ssrn.com/abstract=1013984.

(13) Véase a este respecto el muy explícito Considerando del Tribunal Constitucional alemán: «*The possibility of inspection and of gaining influence has increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed,*

III. LAS LEGISLACIONES DE PROTECCIÓN DE LOS DATOS FRENTE A LOS DESARROLLOS TECNOLÓGICOS

§ 6. ¿El derecho resiste al progreso tecnológico? ¿Puede adaptarse a las evoluciones técnicas para garantizar siempre una protección adecuada para nuestras libertades? La legislación sobre protección de datos personales no escapa a este interrogante. En su caso las reglas sobre la materia, confrontadas a las nuevas tecnologías inteligentes, deberán adaptarse. No se trata de contrariar la esencia de la Ley sino, al contrario, de conseguir que resulte aplicable a los nuevos contextos, en toda su amplitud. En primer lugar deberemos precisar las dificultades para aplicar algunas definiciones clave de la legislación sobre protección de datos de carácter personal a estos contextos nuevos (A), antes de centrarnos en las incertidumbres relacionadas con la aplicación de los principios esenciales de estas legislaciones como la legitimidad, la transparencia o la seguridad del tratamiento de datos (B).

1. Las definiciones frente a las nuevas aplicaciones de la sociedad de la observación

§ 7. Nos vamos a detener sobre algunas definiciones cuyo significado debe reexaminarse bajo las nuevas aplicaciones: la definición de dato de carácter personal (1) está en el centro de controversias recientes. La extensión de la noción de datos sensibles (2) merece igualmente algunas reflexiones, así como la distinción entre el responsable del tratamiento y el encargado del mismo (3), tarea que no es cosa fácil. Por fin, la utilización de los métodos de *profiling* cuestiona el concepto de tratamiento (4).

1.1. La noción de dato de carácter personal

§ 8. Si las personas facilitan su nombre para conseguir una tarjeta de fidelidad o tener la posibilidad de probarse un traje virtualmente, devienen

he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would have also impact the common good ("Gemeinwohl"), because self-determination is an elementary functional condition of a free democratic society based on its citizens' capacity to act and to cooperate».

sin duda identificables y deben aplicarse las reglas relativas a la protección de datos personales. Pero ¿y si las nuevas tecnologías permiten crear perfiles de los individuos o realizar otro tipo de tratamiento sin recoger los nombres u otros datos personales, es decir, sin que resulte aplicable la legislación sobre protección de datos? El análisis del escenario minimalista descrito a propósito del seguimiento de los clientes en el supermercado suscita este interrogante.

§ 9. La aproximación a la noción de dato de carácter personal evoluciona con las nuevas tecnologías y especialmente con los sistemas RFID, que permiten identificar un objeto pero no una persona, aunque es evidente que detrás de la localización del objeto se está apuntando a su poseedor, persona física hacia quien se va a dirigir la decisión. Dado que estas técnicas pueden funcionar sin necesidad de identificar a los individuos, se pueden sugerir dos pistas, si por lo menos se estima que la utilización de estos datos presenta riesgos para las libertades de los individuos. La primera consistiría en extender el concepto de dato personal hacia un sentido más amplio y flexible. La segunda sería regular como tales estos datos que, sin identificar a la persona, permiten individualizarla para tomar decisiones con respecto a ella. La pregunta merece formularse en relación con otros datos, así los registrados mediante *cookies* que no se refieren a un individuo sino a una sesión abierta en un ordenador, en otras palabras, igualmente a un objeto.

En 2007, el Grupo del art. 29 adoptó una opinión sobre el concepto de dato de carácter personal[14] en el sentido de la primera opción. Basándose en la *ratio legis* del legislador europeo, adopta una definición amplia del dato de carácter personal que debe cubrir todas las informaciones que pueden relacionarse con un individuo[15].

Según la definición vista, y según el Grupo de trabajo del art. 29 que se refiere precisamente a un anterior documento de trabajo dedicado a los RFID, si para constituir un dato de carácter personal la información debe predicarse de una persona física identificada o identificable[16], esta noción

(14) Grupo de trabajo «*article* 29» sobre la protección de datos, *Dictamen 4/2007 sobre el concepto de datos personales,* de 20 de junio de 2007, WP 136, disponible en línea.

(15) Véanse las referencias facilitadas por el Grupo del art. 29, precitado, en part. pág. 4.

(16) Según el Considerando núm. 26, «para determinar si una persona es identificable, debe considerarse el conjunto de medios susceptibles de aplicarse razonablemente, bien por

deberá interpretarse no solo en el sentido de que los datos conciernen una persona física «si se refieren a la identidad, a las características o al comportamiento de una persona»[17], sino también cuando «esta información se utiliza para determinar o influenciar la manera en que se trata o se evalúa una persona»[18]. En otras palabras, el dato es de carácter personal, bien por su naturaleza o contexto, que apelan a la posibilidad de identificación, bien por su «finalidad» o «resultado» buscados para tomar una decisión con respecto a una persona aunque no esté identificada o no sea identificable[19]. El elemento finalista consiste en el hecho de que los datos ofrecen a una empresa o una administración la posibilidad de tratar una persona de forma diferente. El elemento de resultado puede definirse, según el Grupo del art. 29, como el impacto provocado por la utilización de los datos para influir sobre el estatuto o el comportamiento de una persona. No es preciso que el impacto sea importante. Basta con que el procedimiento conduzca a tratar un individuo de una manera diferente. Es el caso en el escenario minimalista que acabamos de evocar; es el caso en que, a partir de *cookies*, sociedades de *cybermarketing* como Doubleclick o aún empresas como Amazon pueden dirigir la publicidad que envían e incluso diferenciar las páginas web y los precios fijados en ellas a partir del perfil generado por la utilización de datos registrados mediante *cookies*.

el responsable del tratamiento, bien por otra persona, para identificarla». Así, la dirección IP, incluso en el caso en que la atribución de esta dirección es puramente temporal como ocurre en el marco de la IP v.4, sería un dato de carácter persona. La Corte de casación francesa discute este razonamiento al subrayar con acierto en nuestra opinión, que precisamente según la Ley se prohíbe a los proveedores entregar una información salvo a las autoridades policiales y estima pues que, salvo para la policía, el dato IP no es un dato de carácter personal (Corte de casación, 1 de mayo de 2007 y 27 de abril de 2007). Véase también la decisión de la misma instancia de 13 de enero de 2009, ciertamente más prudente, pero que llega a las mismas conclusiones. Sobre estas decisiones, léase Defraigne, Y. y Escoffier, A. M., «La vie privée à l'heure des mémoires numériques», *Rapport d'information, Commission des lois*, n. 441, 2008-2009, disponible en el sitio del Senado francés: www.senat.fr.

(17) El Grupo del art. 29 pone de relieve el «carácter dinámico» del criterio en el sentido de que la tecnología permitirá identificar a las personas en un instante t+1, cuando no podía hacerlo al instante t.

(18) Grupo de trabajo «art. 29» sobre la protección de datos, *Documento de trabajo sobre cuestiones de protección de datos relacionadas con la tecnología RFID (radio-identification)*, 19 de enero de 2005, WP 105, disponible en línea.

(19) Grupo de trabajo «art. 29» sobre la protección de datos, *Dictamen 4/2007 sobre el concepto de datos personales*, especialmente pág. 11.

§ 10. ¿Debe seguirse la opinión del Grupo del art. 29? Pensamos que no. Esta opinión persigue, desde luego, el loable fin de extender el régimen de protección de los datos de carácter personal, pero esta extensión, además de no respetar la definición de la Directiva, plantea problemas delicados a la hora de aplicar el derecho de acceso que se reconoce al afectado. La persona X a quien se refiere un *cookie* o un *tag RFID*, para acceder a los datos generados por este *cookie* o este *RFID*, deberá empezar por identificarse, justamente cuando hasta este momento no lo estaba —en otras palabras deberá revelar a quien podía seguirla o individualizarla sin identificarla, los datos identificativos que le faltaban—. ¿No sería preferible entonces, tal como sugiere la Directiva 2002/58 llamada *e-privacy*, regular el seguimiento aun sin identificación de las personas aplicando los principios de transparencia y de proporcionalidad[20]?

1.2. *La noción de dato sensible (art. 8)*

§ 11. El consentimiento de la persona afectada se presenta a menudo como el criterio determinante para legitimar los tratamientos de datos sensibles. Nótese, sin embargo, que las leyes internas de los países miembros pueden prohibir el tratamiento de los datos sensibles a pesar del consentimiento de los afectados. No todas las legislaciones son iguales al respecto[21] y esta desigualdad es una muestra de los miedos que suscita esta omnipotencia del consentimiento.

§ 12. Además, ¿qué es un dato sensible? Según nuestra hipótesis, si un cliente adquiere un libro que aborda temas religiosos o sexuales y este producto se registra en su tarjeta de fidelidad y se utiliza para construir su perfil, podría sostenerse que se han tratado datos sensibles. Por otro lado,

(20) Sobre esta idea de una legislación de tercera generación, véase Poullet, Y., «Pour une troisième génération de réglementation de protection des données», en *Défis du droit à la protection à la vie privée*, col. Cahiers du Centre de Recherches Informatique et Droit, 31, Bruxelles, Bruylant, 2008, págs. 25-70. Y más recientemente, del mismo autor: «About the WE-Privacy Directive: Towards a third generation of data protection legislation», en *Data Protection in a Profiled world, Proceedings of the second CPDP Conference*, January 2009, S. Gutwirth, Y. Poullet, P. de Hert (eds.), Springer Verlag, Dordrecht, June 2010.

(21) Léase Cammilleri-Subrenat, A. y Levallois-Barth, C., *Sensitive Data Protection in the European Union*, Travaux du CERIC, Bruylant, 2007, pág. 63.

sería completamente admisible afirmar que la relación entre producto y adquirente no es tan evidente. Ante todo, la gente puede adquirir un determinado artículo con el único fin de informarse acerca de un asunto, sin que esta compra refleje realmente sus gustos personales. Asimismo, los clientes pueden adquirir un producto para otra persona. La apreciación del carácter sensible de un dato depende de la naturaleza del producto y de la transacción[22]. Por ejemplo, un autor revela que, en relación con la naturaleza del producto «*an academic treatise on Satanism will tend to say less about the purchaser's personal religious inclinations than, say, a video-clip depicting satanistic rituals for the purpose of viewer entertainment*»; asimismo en relación con la naturaleza de la transacción: «*a one-off transaction will also tend to say less about the purchaser's personal preferences than a series of transactions involving information products on a similar theme*»[23].

Por añadidura, unos datos que inicialmente no se consideran sensibles podrían convertirse en tales si se recogen y organizan en grandes bases de datos, adquiriendo entonces un fuerte valor económico. Los datos en sí mismos no son sensibles, pero su volumen, y el hecho que puedan venderse por dinero, tienen un impacto sobre sus características[24]. Para acreditar la naturaleza sensible o no debería tomarse en consideración la naturaleza del dato sino, más bien, la naturaleza de su comunicación.

§ 13. Las aplicaciones de las TIC conducen a preguntarse sobre la necesidad de consagrar una nueva categoría de datos sensibles: los identificadores numéricos, los *RFID* insertados en las tarjetas de fidelidades, los *cookies* o la dirección IP. Una evolución notable de los sistemas de información, sean locales o globales, resulta de la disponibilidad y de la utilización de métodos de identificación y de autenticación de los actores/usuarios de los sistemas de información. Estos métodos tanto permiten hacerse conocer o reconocer cuando la «identificación» es condición de acceso a un recurso (*cfr.* los llamados sistemas de *Identity Management*), servicio o una información, como hacerse identificar de forma segura a la hora de sumar, cruzar e incluso deducir datos nuevos sobre uno mismo a partir de elementos de información dispersos en las bases de datos distribuidas en una red sin límites fronterizos[25]. Nótese que estas *digital identities* constituyen entonces metadatos que permiten cruzar las informaciones relativas a una persona residentes en diversas bases de datos[26]. Debe subrayarse el peligro vinculado a la utilización de las *digital identities* comunes a varios sectores de nuestra existencia. Es evidente que cuanto más común sea un método de identificación a numerosas bases de datos, más fácil es el cruce de estas bases de datos. De forma general, este reparto de identificadores entre los responsables de tratamiento plantea de lleno la cuestión de la integridad contextual.

(22) Véase Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, Information Law Series, Kluwer Law International, 2002, núm. 18.4.3, págs. 344-345.

(23) Véase Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.4.3, págs. 344-345.

(24) Véase Bing, J., «Introduction – Notions of sensitive personal data», en *Challenges of privacy and data protection law, Perspectives of european and north american law*, Bruylant, Cahiers du CRID, tomo 31, 2008, págs. 191-208, esp. pág. 195.

1.3. La distinción entre los responsables del tratamiento (art. 2 b de la Directiva), el encargado (art. 2 d) y algunos recién llegados

§ 14. Si por regla general, en lo relativo a la gestión de las tarjetas de fidelidad, el responsable del tratamiento es el comerciante, las operaciones de *profiling* se «subcontratan» a una sociedad que actúa bajo el control del responsable. En efecto, dado que el *profiling* es una actividad muy específica y necesita tanto enormes almacenes de datos, como un *software* que permita descubrir de las inferencias estadísticas, los almacenes están obligados a delegar el análisis de los datos recogidos a sociedades especializadas. Estas sociedades, ¿son simples encargadas en el sentido de la Directiva sometidos al régimen de su art. 17.3? Estas pueden estar interesadas en las plusvalías que ofrece el cruce con datos provenientes de otras fuentes

(25) Son lo que hemos llamado los «*données d'ancrage*», datos de carácter personal que permiten establecer un vínculo entre los datos relativos a un mismo individuo pero localizados en diversas bases de datos. Esta noción se opone a los datos biográficos que describen un elemento de la vida del individuo o lo caracterizan: véase Poullet, y Dinant, J.-M., «L'autodétermination informationnelle à l'ère de l'Internet», Rapport *para el Consejo de Europa*, Nov. 2004.

(26) Sobre estos peligros, véase Rundle, M.C. y Trevithick, P., «Interoperability in the new Digital Identity Infrastructure» (Feb. 13, 2007) *paper* publicado en *Social Science Research Network*, disponible en el sitio web: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962701; Rundle, M. C., «International Personal Data and Digital Identity Management Tools», Research Publication Paper, *The Berckman Center for Internet and Society*, núm. 2006, junio de 2006, disponible en el sitio: http://cyberlaw.law.harcvard.edu/publications.

(p. ej. los datos estadísticos sobre las rentas de la población analizada, las preferencias expresadas con respecto a otros servicios, etc.) e incluso en la venta de los perfiles a otras sociedades. En el tal caso, estaremos ante dos responsables del tratamiento que podrían quedar obligados solidariamente según el art. 2 b.

§ 15. A este dúo cabe añadir la intervención del operador o creador del sistema de información así como el fabricante de los terminales. La noción de «terminal» está definida en la Directiva europea sobre equipos terminales[27] de la siguiente forma: «un producto que permite la comunicación, o un componente pertinente de un producto, destinado a ser conectado directamente o indirectamente por un cualquier medio a las interfaces de las redes públicas de telecomunicaciones (a saber redes de telecomunicaciones que sirven totalmente o en parte para suministrar servicios de telecomunicaciones accesibles al público)». Esta definición muy amplia permite englobar no solo los ordenadores personales, los terminales clásicos como el teléfono, móvil o no, el fax u otros, sino igualmente la televisión interactiva, los *RFID* (*Radio Frequency Identifiers*)[28] las tarjetas *smart*[29] y mañana, las moléculas «inteligentes» implantadas en el mismo cuerpo de los individuos. El reciente debate europeo sobre los *RFID* ha conducido a la Comisión Europea a emitir la Recomendación de 12 de mayo de 2009[30] que afirma la responsabilidad

(27) Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, DOCE núm. L 091 de 07/04/1999 págs. 0010 – 0028.

(28) Estos terminales que son los *RFID* poseen los elementos siguientes:
— un procesador;
— una memoria muerta;
— una antena que permite, a la vez, comunicar con un terminal y recibir la energía requerida para hacer funcionar el ordenador;
— ausencia de periféricos de entrada/salida accesibles a un ser humano;
— muy alto grado de miniaturización (del orden de algunos milímetros, antena incluida).
Sobre los *RFID*, consúltese el sitio muy completo: http://www.rfida.com/nb/identity.htm.

(29) Ciertas tarjetas *smart* están equipadas con procesadores tan potentes como los célebres Apple de principio de los años 80.

(30) *Recomendación sobre la aplicación de los principios de vida privada y de protección de datos de carácter personal*, C (2009) 3200 final. Sobre esta recomendación, léanse las reflexiones de Poullet, Y., «About the WE-Privacy Directive: Towards a third generation of data protection legislation», en *Data Protection in a Profiled world, Proceedings of the second CPDP Conference*, January 2009, S. Gutwirth, Y. Poullet, P. de Hert (eds.), Springer Verlag, Dordrecht, junio 2010.

de los constructores de equipos terminales y de los proveedores de los sistemas *RFID*, es decir, de las infraestructuras que engloban tanto los sistemas de registro, de transmisión de datos engendrados por los terminales *RFID* como las bases de datos en las que estos datos serán analizados y gracias a las cuales se van a tomar las decisiones *ad hoc*. Esta ampliación de la protección de los datos a una regulación de las infraestructuras y de los terminales es indispensable. ¿Cómo asegurar la protección de los datos de forma efectiva si las soluciones técnicas no toman en consideración estas exigencias y las traducen eficazmente? Así, retomando el ejemplo de los RFID, es deseable, de acuerdo con el Grupo del art. 29[31], permitir que el portador del *chip* pueda desactivarlo fácilmente y que el sistema de transmisión utilice soluciones de criptografía. Esta aproximación llamada *privacy by design*[32], afirmada por la reciente Recomendación europea[33], se basa en una reflexión fundamental traducida por primera vez por los redactores de la Ley francesa de 1978, «*L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*». A partir de este texto, los órganos de protección de los datos han afirmado repetidas veces el principio de la responsabilidad de los proveedores de equipos terminales y de los diseñadores de infraestructuras en relación con los riesgos que la utilización de sus infraestructuras o terminales podían generar con respecto a la protección de los datos de sus usuarios.

En conclusión, el papel de cada uno de estos intervinientes debe determinarse claramente en las cuestiones relacionadas con la responsabilidad. Los contratos entre las partes deben ser muy precisos.

(31) *Working paper on the questions of data protection posed by RFID technology*, 19 de enero de 2005, WP No. 105 disponible en el sitio de la Comisión Europea: http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf

(32) Afirmado por Cavioukan, A., *Commissioner of Data Protection for the Province of Ontario, Canada*, en la introducción de los *Privacy Guidelines for RFID Information Systems*, disponible en el sitio: http://www.ipc.on.ca., «*Privacy and Security must be built in from the Outset – at the design Stage*».

(33) La Recomendación europea invita al operador RFID (tanto el fabricante de terminales como el diseñador del sistema de información) a redactar una memoria sobre el impacto de su sistema o de su terminal sobre la protección de los datos y la vida privada de las personas afectadas por el desarrollo del sistema RFID.

1.4. *La noción de tratamiento respecto a la utilización de las técnicas de* profiling

§ 16. ¿El *profiling* es un tratamiento o un método de explotación de los datos al servicio de un tratamiento? En el escenario propuesto, el *profiling* realizado a partir de las tarjetas de fidelidad de los clientes de los almacenes y de los chips *RFID* tiene por objeto establecer una dinámica marketing *one-to-one*. En otras palabras, no parece que el *profiling* sea *per se* una finalidad más, sino que permite sencillamente conseguir con mayor facilidad la finalidad del tratamiento de marketing. El *profiling* se diferencia de los tratamientos clásicos de datos de carácter personal en la medida que un individuo identificable o identificado ve cómo *in fine* se le atribuyen ciertos datos que no son los suyos, sino los del grupo al que pertenece con mayor o menor probabilidad. Además, el *profiling* se diferencia del tratamiento estadístico en que, aunque incluya operaciones estadísticas, persigue una finalidad distinta. A diferencia del tratamiento estadístico, que no constituye una ayuda para la toma de decisiones individuales sino globales, en materia de *profiling*, la aplicación del resultado de las operaciones estadísticas no tiene por objeto alimentar una decisión global o modificar una línea de acción, sino que es directa e individual. En este sentido, el *profiling* permite una aplicación inmediata de su resultado. Por añadidura, la finalidad podría ser múltiple. Más allá del marketing, permitiría controlar los desplazamientos de los clientes, evitar los robos en los grandes almacenes, determinar la oferta a la clientela e incluso vender los perfiles a de otras sociedades. El *profiling* puede definirse entonces como: «*the interference of a set of characteristics (profile) about an individual person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics. The set of characteristics will typically relate to the behaviour (actual or expected) of a person/entity (...). What is new (...) is the increasingly extensive, systematic use by organisations of relatively formalised and sophisticated profiling practices* ***for a variety of control purposes***»[34]. En definitiva, el *profiling* no es un objetivo en sí

(34) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 17.2, pág. 301. Véase también «Profiling the European Citizen, Cross-Disciplinary Perspectives», M. Hildebrandt and S. Gutwirth (ed.), *op. cit.*; Dinant, J.-M., Lazaro, Ch., Poullet, Y., Lefever N., Et Rouvroy, A., *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee*, Consejo de

mismo sino un medio técnico de conseguir un resultado particular en el contexto de uno o de varios tratamientos[35].

§ 17. Ello no impide que el *profiling*, como, por otra parte, los sistemas de decisiones automatizadas contempladas en el art. 15 de la Directiva[36], constituya una técnica que requiere una protección específica, ya que gracias a ella los tratamientos de datos devienen cada vez más poderosos, si pensamos simplemente en el número creciente de datos tratados o la sofisticación creciente de todos estos procesos[37]. Así, la agregación de datos procedentes de diversas bases de datos permitirá deducir con una tasa de certeza del 89% que la composición de una determinada cesta de compra por un consumidor que se presenta en una gran superficie a determinada hora del día proviene de una persona seguramente soltera, aficionada a los viajes lejanos y defraudador potencial. El perfil del terrorista se deduce del cruce de datos tan diversos como el registro de población, la utilización de tarjetas de crédito, los desplazamientos registrados gracias a los móviles, las tarjetas de fidelidad, el consumo de medicamentos, etc.[38] La disminución drástica de los costes de

Europa, 13/14 de marzo de 2008; Ranse, S., «Le profiling des internautes au regard du droit au respect de la vie privée: le coût de l'efficacité!», *RDTI* 2004, núm. 20. Y recientemente, *Data collection, targeting and profiling of consumers for commercial purposes in online environments*, European Commission, Health and Consumers Directorate-General, Bruxelles, 5 de marzo de 2009.

(35) Véase Dinant, J.-M., Lazaro, Ch., Poullet, Y., Lefever, N. y Rouvroy, A., *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee*, *op. cit.*, esp. pág. 32.

(36) Véase Dinant, J.-M., Lazaro, Ch., Poullet, Y., Lefever N. y Rouvroy, A., *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee*, *op. cit.*, esp. pág. 32.

(37) Véase Dinant, J.-M., Lazaro, Ch., Poullet, Y., Lefever, N. y Rouvroy, A., *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee*, *op. cit.*, esp. pág. 33. Los autores prosiguen: «*Without such protective arrangements, there is a significant risk that commercial undertakings will make increasing and systematic use of rapid and inexpensive profiling of their customers. Such profiling will inevitably result in certain individuals being excluded from particular goods or services or having to pay a higher price for them*». Véase asimismo la excelente obra que reúne artículos sobre el tema del *profiling*, editado por Hildebrandt, M. y Gutwirth, S., «Profiling the European citizen, Cross disciplinary Perspectives», *op. cit.*

(38) Sobre las aplicaciones del «*data mining*» en materia de seguridad pública léase Solove, D. J., «Data Mining and The Security – Liberty Debate», 75 *University Chicago Law Review*, 2008, pág. 343 y ss. El autor evoca en particular el programa americano Matrix (*Multistate Anti-Terrorism Information Exchange*).

almacenamiento, la sofisticación de las herramientas de análisis de datos y el poder de cálculo de nuestros ordenadores permiten estos cruces aleatorios de los que surge la verdad, al menos estadística, de los perfiles que resta por confrontar con los datos relativos a personas particulares. En suma, el ciudadano ve cómo se le aplica el resultado de un conocimiento deducido de este perfil construido a partir de datos que no lo conciernen, que a menudo tiene poca relación lógica con la operación para la que se utiliza el perfil y que le resultan ampliamente desconocidas. Peor aún, este perfil confiere al responsable del tratamiento un mejor conocimiento de la persona afectada que el que pueda tener ella misma y, si esta persona argumenta que este perfil no le conviene, o que, en cualquier caso la decisión que se le aplica es errónea, deberá probar el error[39].

§ 18. Tal como hemos dicho, el *profiling* permite tomar decisiones automatizadas. ¿Debe aplicarse entonces el art. 15 de la Directiva 95/46, relativo a las decisiones individuales automatizadas?

En virtud del art. 15, todo individuo tiene «derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.». Esta disposición «*restricts a particular* application *of a particular type of profiling process. It does not directly restrict the* creation *of profiles*»[40]. En efecto, deben satisfacerse cuatro condiciones para que el sistema de decisión automatizada caiga bajo la aplicación del art. 15. Ante todo debe tomarse una decisión. Luego, esta debe producir efectos jurídicos significativos sobre el individuo. La decisión debe resultar de un tratamiento automatizado de datos. Finalmente es necesario que los datos se traten con el fin de evaluar ciertos aspectos del individuo como su comportamiento, sus preferencias o sus necesidades[41].

(39) Sobre esta inversión de la carga de la prueba inducida por el *profiling*, léase Steinbock, D. J., «Data Matching, Data Mining and Due Process», 40 *GA Law Rev* (2005), 1, págs. 82 y ss.

(40) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 319.

(41) Sobre todos estos puntos, véase Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 319.

¿Qué es un «efecto jurídico que afecte de manera significativa» un individuo? ¿Debe aprehenderse en un sentido objetivo, sin tomar en consideración las percepciones particulares de las personas afectadas? ¿Los efectos pueden ser económicos? ¿O acaso son solo económicos? *A priori*, el envío de publicidad individualizada por ejemplo no entra en esta categoría. Sin embargo, los considerandos 9, 10 y 23 invitan a tomar en consideración los efectos materiales e inmateriales de este tipo de decisiones. Además, si se considera que el art. 15 contempla la protección de la integridad y de la dignidad de los individuos frente a un mundo cada vez más automatizado, las percepciones propias de las personas deberían tomarse en cuenta. Lo que no impide preocuparse, igualmente, por un número considerable de otros individuos para fundar la reflexión sobre una base razonable[42]. Además, los efectos generados deben ser contrarios a los intereses de la persona. Es cierto que la disposición no menciona esta restricción; pero sería sin duda extraño que el art. 15 pudiera aplicarse a una decisión que produce efectos positivos sobre el individuo. Así pues, un «efecto significativo» solo puede entenderse como un «efecto significativo contrario»[43].

Por ejemplo, el envío de un folleto a una lista de personas seleccionadas sobre la base de un procedimiento automatizado no puede considerarse como algo que las afecte significativamente y en todo caso no de forma negativa. En cambio, ciertos tipos de publicidad tienen la facultad de provocar efectos contrarios significativos sobre los individuos, cuando la selección es tal que permite una manipulación de estos últimos. Por otra parte, cuando el procedimiento tiende a operar una discriminación desleal entre los clientes, el efecto producido puede ser significativo[44]. Por ejemplo, si ciertos productos se ofrecen a la venta a un precio superior a ciertos

(42) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 322: «*the legal weight of the perception will depend on the extent to which it is regarded by a considerable number of other persons as having a reasonable basis*».

(43) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 323.

(44) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 323. Véase también Dinant, J.-M., Lazaro, Ch., Poullet, Y., Lefever, N. y Rouvroy, A., «Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee», *op. cit.*, esp. pág. 14.

consumidores, o si a algunos se les impide comprar un tipo de producto a diferencia de la mayoría de clientes, estas prácticas son susceptibles de provocar efectos negativos significativos sobre aquellos. No es incongruente imaginar que el precio de un producto pueda ser directamente proporcional a los hábitos y preferencias del consumidor. En la medida que el *profiling one-to-one* permite conocer y ofrecer pues servicios personalizados a los clientes, ¿por qué privarse de una adaptación personalizada de los precios? Con la llamada técnica de *dynamic pricing*, los responsables del tratamiento «*can judge with greater accuracy than the consumer may know, the latter's willingness to pay for a particular product, based on past behaviour*»[45].

En definitiva, ¿debe ser extensa la interpretación del art. 15? En algunos casos sería posible argumentar que el simple hecho de ser juzgado por una máquina debe interpretarse como un insulto a la dignidad del individuo, lo que conduciría a atribuir, en todo caso, a tal decisión un efecto significativo[46]. Debería entonces considerarse que «*the simple fact of individual's being subjected to automated profiling to assess certain aspects of their personality should be sufficient by itself to entitle them to be informed of this profiling and of its underlying logic, and to challenge it, at least in certain cases of automated processing deemed to be capable of making such assessments*»[47] y someter a una reglamentación específica las actividades de *profiling* aun fuera del art. 15 de la Directiva.

2. Los principios

§ 19. Seguidamente se detallan las cuestiones suscitadas a propósito de algunos principios: lealtad y transparencia (1), legitimidad (2), proporcionalidad (3), así como seguridad (4).

(45) *Data collection, targeting and profiling of consumers for commercial purposes in online environments*, European Commission, health and Consumers Directorate-General, Bruselas, 5 de marzo de 2009, esp. pág. 12.

(46) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 322.

(47) Dinant, J.-M., Lazaro, Ch., Poullet, Y., Lefever N. y Rouvroy, A., *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee*, *op. cit.*, esp. pág. 34.

2.1. El principio de lealtad y de transparencia

§ 20. El art. 6.1 de la Directiva 95/46/EC exige lealtad en el registro de los datos y el tratamiento. Esta prescripción de recogida leal implica que la persona esté informada cada vez que se recolectan sus datos. El funcionamiento de los sistemas RFID, vista la dimensión del terminal e incluso su funcionamiento invisible por un lado, y las modalidades de registro vinculadas a internet por otro, justifica la particular atención otorgada a este primer principio. Una primera obligación se desprende de las opiniones del Grupo del art. 29 en materia de RFID y se consagra en la Recomendación mencionada *supra*[48]: se trata de la obligación de dar transparencia a la presencia de los RFID, incluso mediante una etiqueta. Por añadidura, como hemos subrayado, estas modalidades de registro van más allá de lo que se pueda considerar «expectativas razonables» de la persona. Así, aunque esta conozca la existencia del *chip* RFID, ¿puede imaginar que este *chip* permitirá registrar sus desplazamientos, sus indecisiones delante de diversos productos, que el registro no se limita a una sola visita sino que cubre el conjunto de las visitas a los almacenes de la cadena y que esta memoria permite un *profiling* exhaustivo?

El art. 10 de la Directiva se hace eco a este imperativo de lealtad obligando al responsable del tratamiento a suministrar la información necesaria sobre el nombre del responsable, las finalidades, los terceros a quienes se van a comunicar los datos y la existencia del derecho de acceso. El artículo añade que este deber de información debe extenderse a toda información necesaria para garantizar el carácter leal del tratamiento en función de las circunstancias particulares de este. Este añadido encuentra todo su sentido en la utilización de estas nuevas tecnologías, cuyo funcionamiento es opaco. Es importante que las personas cuyos datos van a almacenarse sobre los *chips* RFID estén al corriente no solo del registro de todos estos datos, sino de la aplicación de las técnicas de *profiling* sobre los mismos.

§ 21. El derecho de acceso, de corrección o de complemento proclamados por el art. 12 de la Directiva prolonga este deber de transparencia del responsable del tratamiento. El art. 12 prevé que este derecho abarca no solo el acceso a los datos captados, sino también a las informaciones que

(48) *Cfr. supra* n. 15.

resultan del tratamiento y, en caso de decisión automatizada, a la lógica del sistema[49]. En la medida que los *profilings* aludidos en los escenarios mencionados constituyen sistemas automatizados de decisión, aunque *in casu* su alcance (envío de publicidad o ajuste de precio) sea insuficiente para que juegue el art. 15 de la Directiva relativo a estos sistemas automatizados de decisión[50], estimamos que la disposición que prevé el derecho de acceso a la lógica debería aplicarse en vistas a la generalización del uso de técnicas de *profiling* y de los riesgos de manipulación de los individuos que conllevan. En otras palabras, la persona a quien se opone un perfil debería poder conocer la «lógica» ciertamente aleatoria pero muy presente, que ha permitido establecer el perfil. Saber que se me recomienda tal o cual producto porque mis compras anteriores me ordenan en una categoría determinada es, en nuestra opinión, una exigencia si es que se desea —lo que constituye el fin del derecho de acceso— permitir a la persona encontrar cierto equilibrio informativo en su relación con los responsables de tratamiento. Es sobre la base de este conocimiento que la persona afectada podrá, en su caso, rectificar el juicio ajeno fundado en la aplicación automatizada del perfil u oponerse a la continuación de su *profiling*.

Sin embargo, este derecho de acceso no es absoluto. Supone que el responsable pueda conocer esta lógica. Luego, esta debería estar disponible, documentada, presta a ser consultada. La documentación debe contener información sobre las categorías de datos tratados y sobre su papel en el desarrollo de decisiones[51]. Por otro lado, es completamente probable que el método de *profiling* constituya un *know how*[52] que el responsable del tratamiento o su encargado opondrán a la petición de acceso del afectado. En efecto la sociedad encargada de esta actividad desarrolla ciertamente sus propios medios técnicos o algoritmos para realizar de los perfiles de alta calidad. Su éxito depende de sus competencias particulares. El *know*

(49) El derecho de acceso incluye «el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del art. 15» [art. 12 a) de la Directiva].

(50) *Cfr. infra* n. 18.

(51) Lee Bygrave, A., *Data Protection Law, Approaching Its Rationale, Logic and Limits*, *op. cit.*, núm. 18.3.1, pág. 325.

(52) Sobre el tema véase en particular *Le Know How, 5ème rencontre de Propriété industrielle*, Travaux de la Faculté de droit er des sciences économiques de Montpellier, Librairies techniques, Actualités de droit de l'entreprise, T. 7, 1976.

how tiene un valor económico importante y se mantiene pues secreto. La empresa no ostenta un derecho privativo sobre el *know how*. Sin embargo, este se protege por dos vías. La competencia desleal es una de ellas, en caso de que un individuo tuviera la intención de revelarlo a otras sociedades sin autorización, o si un competidor la roba entregándose al espionaje industrial. Igualmente, la revelación de secretos se reprime penalmente. Existe una situación semejante en derecho de la competencia cuando se concede al individuo implicado en un procedimiento en la materia el derecho de acceso a los expedientes de la Comisión para garantizar el principio de igualdad de medios[53]. De hecho, aunque este derecho de acceso esté consagrado en diferentes textos de la Comunidad Europea, solo puede ejercerse respetando la protección conferida al secreto de los negocios[54]. En conclusión, el derecho de acceso queda, a nuestro parecer, limitado por todo lo que sea estrictamente necesario para mantener el secreto de los negocios[55].

2.2. *El principio de legitimidad de las finalidades perseguidas por el registro de los datos*

2.2.1. El *profiling* y la cuestión de la finalidad legítima y/o compatible (art. 6)

§ 22. Lo que nos interesa es el tratamiento ulterior que podría hacerse con los datos. Solo es aceptable un tratamiento que respete las mismas finalidades que el tratamiento original; si los fines son incompatibles, el tratamiento queda prohibido o mejor dicho debe encontrar una base de legitimidad propia, al no poder apoyarse sobre la legitimidad del tratamiento de base. Para saber si una finalidad es compatible o no con la de origen,

(53) Véase Cammilleri-Subrenat, A. y Levallois-Barth, C., *Sensitive Data Protection in the European Union*, *op. cit.*, pág. 43.

(54) Art. 27 (1) y (2) de la Recomendación del Consejo (EC) núm. 1/2003 de 16 de diciembre de 2002 sobre la aplicación de las reglas de competencia de los arts. 81 y 82 del Tratado de la UE. Véase Cammilleri-Subrenat, A. y Levallois-Barth, C., *Sensitive Data Protection in the European Union*, *op. cit.*, págs. 43-44.

(55) Art. 15 (1) y (2) del Reglamento (CE) núm. 773/2004 de la Comisión, de 7 de abril de 2004, relativo al desarrollo de los procedimientos de la Comisión con arreglo a los arts. 81 y 82 del Tratado CE. Véase Cammilleri-Subrenat, A. y Levallois-Barth, C., *Sensitive Data Protection in the European Union*, *op. cit.*, págs. 43-44.

es preciso referirse al criterio de la *reasonable expectation* de las personas afectadas. La pregunta que podríamos plantear en este contexto es la siguiente: ¿los individuos están en condiciones de suponer, al principio del proceso de tratamiento de datos, que estos podrán tratarse de otra manera? Más específicamente, el objetivo inicial del tratamiento de datos —las tarjetas de fidelidad por ejemplo— ¿incluye el *profiling*? En caso de respuesta positiva, el nuevo procedimiento es compatible con el primero y, luego, no es preciso cumplir ninguna formalidad suplementaria. Pero en caso de respuesta negativa, el procedimiento debe satisfacer todas las reglas requeridas por la Ley para ser legítimo.

§ 23. La exigencia de compatibilidad solo se aplica al fin del tratamiento de datos. Y en la medida en que el *profiling* no constituye una finalidad sino un método de tratamiento, la cuestión del *reasonable expectation* no debe plantearse en términos de legitimidad sino, en su caso, tal como ya hemos afirmado en materia de lealtad o de transparencia[56] y de proporcionalidad[57]. En efecto, la técnica del *profiling* se pone al servicio de la finalidad *marketing* que puede encontrar su legitimidad bien en el art. 7 f), de la Directiva, bien en el consentimiento de las personas afectadas. Este segundo fundamento es el objeto de las reflexiones siguientes; digamos una palabra a propósito del primer fundamento. El art. 7 h), exige poner en una balanza los intereses del responsable del tratamiento: los del tercero a quien se van a comunicar los datos, por un lado, y los de la persona afectada, por otro. Está claro que la utilización de los métodos de *profiling* influirá sobre esta balanza en la medida en que, como se ha dicho, el *profiling* conlleva riesgos suplementarios para la persona afectada. Así, si la utilización de las técnicas sofisticadas de *profiling* que permite un marketing *one-to-one* no plantea problemas de compatibilidad, sin embargo nos parece que plantea un tema delicado de legitimidad de tratamiento en relación con el art. 7 h)[58].

(56) *Cf. supra* n. 20.

(57) *Cf. infra* n. 25.

(58) Como indica la memoria sobre los aspectos jurídicos y éticos y sociales redactada en el marco del proyecto MIAUCE, «*it's true that this possibility [public interest] is often advanced by marketers to justify their processing: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject...". They argue that their interest as marketers is legitimate and that the prejudice they cause to the data subject is minor*

Así pues, la sola hipótesis que puede legitimar el tratamiento de datos en el contexto de tarjetas de fidelidad o de *profiling* sigue siendo el consentimiento inequívoco prestado por los clientes. Esta es igualmente la opinión del Grupo del art. 29: «en la mayoría de los supuestos en que se utiliza la tecnología RFID, el consentimiento de las personas será el único motivo legal que podrán invocar a los responsables del tratamiento de datos para legitimar el registro de informaciones por radio-identificación. Por ejemplo, un supermercado que marca de las tarjetas de fidelidad o bien deberá explicitar las reglas contractuales, o bien obtener el consentimiento de la persona para relacionar la información personal conseguida en el contexto de la entrega de la tarjeta de fidelidad con la información registrada mediante la tecnología RFID»[59].

2.2.2. La presunción de legitimidad de los tratamientos de datos por el consentimiento

§ 24. El art. 7 de la Directiva prevé que «el tratamiento de datos personales solo pueda efectuarse si a) el interesado ha dado su consentimiento de forma inequívoca». El hecho de que el consentimiento deba ser indudable sugiere que no puede ser sencillamente implícito. Así, los sistemas *opt-in* deben preferirse a los de tipo *opt-out*. Además, el consentimiento solo es válido si es libre, es decir prestado sin coacción física o psicológica, específico para un tratamiento determinado e informado, lo que supone que la

in comparison with the benefits the data subjects will get from the publicity and with their own legitimate interests. As the value behind data protection is the fundamental right to privacy, including the right not to undergo excessive pressures and constrains in the autonomous development of one's personality, and that individualized marketing and advertising may come to be so effective that it may indeed exercise such an excessive pressure, the marketers' argument does not appear sufficient to justify in all cases such data processing. The legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed may legitimize the processing as long as these interests are not overridden by interests for fundamental rights and freedoms of the data subject. A balance must therefore be made between the data controller's and the data subject's interests. The more the processing infringes upon the data subject's fundamental liberties and freedoms, the less probable it is that the processing will appear legitimate».

(59) Grupo de trabajo «art. 29» sobre la protección de datos, *Documento de trabajo sobre cuestiones de protección de datos relacionadas con la tecnología RFID (radio-identification)*, de 19 de enero de 2005, WP 105, disponible en línea.

persona haya sido informada del tratamiento de datos. ¿Cómo puede considerarse indudable este consentimiento en el marco de nuestro escenario?

Un consentimiento es válido si se cumplen tres condiciones. En primer lugar debe ser libre. Es inconcebible que el profesional ejerza cualquier presión sobre los clientes. Por ejemplo, privarlos de los consejos de un vendedor si rechazan una tarjeta de fidelidad es una coacción que impide la libertad del consentimiento Rechazar una tarjeta de fidelidad o ser sometido a *profiling* no debería conllevar a una desventaja al cliente, cosa que, como hemos visto[60], está lejos de ser evidente. Luego, el consentimiento debe ser específico. Eso significa que cada tratamiento de datos necesita el acuerdo de las personas. Ciertamente, hemos visto que el *profiling*, entendido como técnica de tratamiento y no como finalidad, no exigía el consentimiento por parte de los clientes. Sin embargo, el desarrollo exponencial de esta práctica combinada con los riesgos subyacentes que genera ha conducido a predicar la necesidad de una reglamentación específica. Por ello, para la coherencia de nuestra argumentación, aunque la Ley no exija (aún) el consentimiento de los individuos para el *profiling*, parece oportuno que tenga que prestarse el consentimiento tras una información diligente sobre su existencia y los métodos utilizados. Debe alentarse este comportamiento voluntario por parte de los responsables del tratamiento. Finalmente, el consentimiento debe ser informado. Los comerciantes deben dar a sus clientes, de forma comprensible, toda la información sobre el tratamiento de datos para que puedan prestar su consentimiento con conocimiento de causa. Además, el consentimiento debe ser revocable. Los clientes deben estar en posesión de los medios técnicos que permiten borrar los datos registrados en las tarjetas de fidelidad que sirven para establecer su perfil.

2.2.3. La proporcionalidad de los datos tratados y conservados

§ 25. El art. 6 c) de la Directiva afirma que los datos registrados y utilizados deben ser «adecuados, pertinentes y no excesivos», en relación con las finalidades perseguidas. Este principio de proporcionalidad de los datos respecto a las finalidades prohíbe igualmente conservar los datos más allá

(60) *Cfr. supra* núm. 2 donde se tratan en particular las facilidades obtenidas gracias a la carta de fidelidad, como la posibilidad de cobro rápido por caja y sobre todo las facilidades en materia de garantía.

del tiempo necesario para alcanzar la finalidad. Así, registrar la dirección de la persona cuando entrega de la tarjeta de fidelidad es ciertamente necesario si a ella se vincula la posibilidad de garantías sobre los productos adquiridos o de servicio a domicilio. Podría serlo menos en otros casos. Por ejemplo, recabar datos sobre la situación familiar (número y edad de los hijos) no parece indispensable. Más aún, ¿podemos considerar proporcionado a los fines de marketing personalizado, el registro sistemático de los recorridos por el interior de una gran superficie? De manera más fundamental ¿puede conciliarse el respeto a la proporcionalidad en el marco del uso de estas técnicas de marketing con el registro y el tratamiento de cualquier dato con el argumento de que esta técnica publicitaria lo exige? La misma reflexión cabe a propósito de la duración cuando el registro de los datos se justificada por la concesión de una garantía al comprador de un producto: ¿puede considerarse que es necesaria la conservación de este dato a lo largo de toda la duración de la garantía, incluso o a lo largo de varios años?

La aplicación de este principio plantea todavía más dificultades en el marco de las operaciones de obtención de perfiles. En efecto, estas operaciones se caracterizan por el descubrimiento de correlaciones estadísticas no necesariamente predecibles. La presencia y la combinación de determinados productos en la cesta de quien hace sus compras a las 6 de la tarde y ha dado sus medidas en línea, revela una persona sensible a los productos de países lejanos y propensa a gastos irreflexivos. A diferencia de otros tratamientos donde el carácter necesario de un dato puede analizarse *a priori* por el examen de la finalidad y el vínculo lógico que existe entre el tratamiento un dato determinado y la persecución de esta finalidad, en el caso del *profiling*, la relación de necesidad se descubre *a posteriori* por el descubrimiento de inferencias estadísticas insospechadas al principio. Desde luego, se puede exigir la codificación de los datos: «tal consumidor se convierte en el Sr. X» pero aunque esta codificación da cierta seguridad al proceso, en particular si lo opera una tercera empresa, no impide que el dato continúe siendo un dato de carácter personal.

2.2.4. El principio de seguridad

§ 26. La Directiva, en su art. 17 § 1, obliga al responsable del tratamiento a tomar de las medidas de seguridad apropiadas, tomando en considera-

ción en particular los riesgos que podrían presentar la falta de integridad, de disponibilidad y de confidencialidad de los datos tratados y teniendo en cuenta los riesgos que presente el sistema de información de registro y de tratamiento.

El escenario analizado llama la atención sobre las particularidades de los sistemas de información utilizados. En efecto, se basan sobre terminales que permiten el registro pero constituyen igualmente bases de datos; así la tarjeta de fidelidad provista de un *chip* RFID emite información sobre la situación de los consumidores pero puede registrar igualmente los datos generados por las compras sucesivas de productos, el momento, el nombre de la cajera, el lugar, etc.[61]. Nótese igualmente que en el escenario se utilizan infraestructuras de comunicación, un *intranet* que enlaza el conjunto de los chips RFID dispersos en el almacén y también internet. La presencia de estos terminales y la transmisión por estas redes de comunicación multiplican los riesgos. Así, cabe imaginar en particular la lectura a distancia del contenido del *chip* RFID del consumidor. La seguridad de los datos toma pues una nueva dimensión y obliga a extenderse a nuevos actores. Así, quienes conciben o producen el terminal deben asegurar el acceso al *chip* RFID, encriptar automáticamente las comunicaciones procedentes de ellas, etc. Quienes conciben los sistemas de información que permiten tanto el registro como la transmisión de los datos deben velar para que las interceptaciones de comunicación no sean posibles y no puedan introducirse aplicativos espía en el terminal de la persona afectada. Estas nuevas obligaciones aparecen claramente en la recomendación europea y la opinión del Grupo del art. 29[62].

3. Las tecnologías inteligentes desde el prisma de la legislación sobre prácticas comerciales desleales

§ 27. El marketing al que nos enfrentamos ya no es un marketing de masas, sino un marketing personalizado o, dicho de otra manera, un mar-

(61) Para un análisis en particular en materia de seguridad, nos remitimos al artículo: «Les cartes sans contact: une comparaison de trois utilisations en billetique», por Denis Darquennes, físico, informático e investigador senior del CRID, bajo la supervisión del Profesor Yves Poullet, Director del CRID, Profesor ordinario en la Facultad de Derecho de Namur.

(62) Ya citadas y comentadas, *supra* n. 15.

keting *one-to-one*[63]. La tendencia ha evolucionado en el sentido de una «toma de conciencia del valor individual de un cliente»[64]. El *leitmotiv* ya consiste en seguir las necesidades del consumidor, sino avanzarse a ellas. Además, este necesita connivencia para ser fiel. El registro de datos referentes a su consumo se revela entonces indispensable para «reconstituir lo más fielmente posible la relación individual que nace con el comerciante de proximidad»[65]. Ya no es el momento de establecer «artefactos» estadísticos que no corresponden a ningún individuo en particular, sino de encontrar al hombre que existe detrás del artefacto[66]. En efecto, «la apuesta del *one-to-one* consiste en pasar de la abstracción del consumidor a la realidad del persona»[67]. Y justamente ahí reside el problema. El conocimiento del individuo que pueden adquirir los profesionales del marketing no parece tener límites. El objetivo consiste en aproximarse lo máximo posible al sentimiento humano para poder proponer luego productos o servicios adaptados. La manipulación ya no queda quizás demasiado lejos. La aproximación a estas tecnologías inteligentes bajo el ángulo de las reglas que rigen las prácticas de marketing merece algunas consideraciones.

§ 28. El texto de referencia en la materia es la Directiva 2005/29/CE del Parlamento y del Consejo del 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas con respecto a los consumidores en el mercado interior[68]. Se trata de una «directiva-marco que cubre el conjunto de las prácticas desleales que afectan a los consumidores»[69]. La

(63) Expresión encontrada por Rogers, M. y Peppers, D., *Le One-to-One, Valorisez votre capital-client*, Editions d'Organisation, 1998.

(64) Véase Girot, J.-L., «Pourquoi l'entreprise doit-elle développer sa connaissance des clients?», en *Le harcèlement numérique*, Institut Présage, Dalloz, 2005, págs. 51-73, esp. pág. 55.

(65) *Ibid.*

(66) Lemoine, Ph., «Commerce électronique, marketing et liberté», en *La protection de la vie privée dans la société de l'information*, Pierre Tabatoni (director), Tomo 2, PUF, 2002, págs. 9-23, esp. pág. 15 y ss.

(67) Pensamiento de Pepper y Roggers resumido por Barchechath, E., «Une lecture critique du One-to-One», en *Commerce électronique, Marketing et Libertés*, Cahier LASER núm. 2, Laser, 1999, págs. 87 a 104, esp. pág. 98.

(68) Esta Directiva modifica la Directiva 84/450/CEE del Consejo y las Directivas 97/7/CE, 98/27/CE y 002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) no 2006/2004 del Parlamento Europeo y del Consejo.

(69) Calais-Auloy, J. y Steinmetz, F., *Droit de la consommation*, Dalloz, Précis Droit privé, 7.ª ed., 2006, núm. 80-2, págs. 89-90.

Directiva 2005/29 opera una armonización total —contrariamente a las directivas anteriores que exigían solo una armonización mínima— en el sentido que la protección de los consumidores a escala nacional no podrá ser inferior ni superior a la propuesta por la directiva[70]. La publicidad y el marketing no son objeto de un tratamiento específico por la directiva. Asimismo, sitúa en el mismo plano a este tipo de actos y cualquier otra actividad vinculada con la promoción o la venta de productos a los consumidores[71]. Las acciones de marketing dirigidas a los consumidores entran pues en el campo de aplicación de la directiva. La noción de práctica comercial se beneficia de una aproximación generosa al definirse como todo acto, omisión, conducta o manifestación, o comunicación comercial, incluidas la publicidad y la comercialización, procedentes de un comerciante y directamente relacionados con la promoción, la venta o el suministro de un producto a los consumidores[72] [73]». Tales prácticas serán desleales si «*it deemed to be unacceptable with regards to the consumer, according to specified criteria*[74]». El Considerando n.° 8 pone el acento sobre la protección de los intereses económicos de los consumidores contra las prácticas comerciales desleales de las empresas, con exclusión de otros intereses como la salud o la seguridad[75].

§ 29. El contexto del marketing se estudiará bajo el ángulo de la legislación protectora de los consumidores (A). Este paso, centrado en la legislación protectora de los consumidores, no se limitará a una aproximación bajo el ángulo de las disposiciones sobre protección de datos personales. Las dos legislaciones pueden, desde luego, estudiarse en paralelo pero parece posible proponer una reflexión «integradora», en el sentido que una infracción de la legislación relativa a los datos personales podría constituir una práctica comercial desleal en el sentido de la directiva 2005/29. La violación de la legislación sobre los datos personales por las empresas podría en si misma emparentarse a una práctica comercial desleal hacia los consumidores (B). La aproximación parece interesante, sobre todo si se tiene en cuenta que estos argumentos ya han sido utilizados por empresas en contra de otras empresas competidoras.

(70) Calais-Auloy, J. y Steinmetz, F., *Droit de la consommation*, *op. cit.*, núm. 80-2, pág. 90.

(71) El Considerando núm. 7 precisa que «La presente Directiva aborda las prácticas comerciales que influyen directamente en las decisiones de los consumidores sobre transacciones relacionadas con productos».

(72) *Cf.* Considerando núm. 7.

(73) Art. 2 d) de la Directiva 2005/29. Compárese con el art. 2 f) de la Directiva 2000/31, de 8 de junio de 2000, sobre el comercio electrónico.

(74) «The Unfair Commercial Practices Directive, Questions and Answers», *European Commission, Press release*, 12 de diciembre de 2007, disponible en línea.

(75) *La directive relative aux pratiques commerciales déloyales*, Direction générale Santé et protection des consommateurs, Commission européenne, 2006, esp. pág. 18.

3.1. *Las prácticas comerciales desleales en el sentido de la Directiva 2005/29*

§ 30. Para saber si una práctica comercial entra en el ámbito de aplicación de la Directiva 2005/29, conviene ante todo comprobar si forma parte de la lista negra promulgada por la Directiva (1). Si no es así, es preciso plantearse si entra en la definición de una práctica comercial agresiva (2) o de una práctica comercial engañosa[76]. Si la práctica comercial no corresponde a ninguna de estas definiciones, la reflexión se orientará hacia el art. 5 que proscribe las prácticas comerciales desleales que no son agresivas ni engañosas (3).

3.1.1. Lista negra de las prácticas comerciales desleales en toda circunstancia

§ 31. La Directiva 2005/29 ha establecido una lista negra de las prácticas desleales en toda circunstancia[77] (anexo 1), sin referirse al test del consumidor medio[78]. No es necesario evaluar los casos uno por uno. Se incluyen en esta lista, como prácticas comerciales agresivas, el hecho por ejemplo de:

> «24) Crear la impresión de que el consumidor no puede abandonar el local hasta haber perfeccionado el contrato.
>
> 25) Realizar visitas en persona al domicilio del consumidor, ignorando las peticiones de este de que el comerciante abandone su casa o no vuelva a personarse en ella, salvo en las circunstancias y en la medida en que esté

(76) No abordaremos aquí las prácticas comerciales engañosas (art. 6 y ss. de la Directiva 2005/29).

(77) Nos remitimos al Considerando núm. 17 de la Directiva 2005/29.

(78) *Cfr. infra*.

justificado, con arreglo a la legislación nacional, para hacer cumplir una obligación contractual[79].

26) Realizar proposiciones no solicitadas y persistentes por teléfono, fax, correo electrónico u otros medios a distancia, salvo en las circunstancias y en la medida en que esté justificado, con arreglo a la legislación nacional, para hacer cumplir una obligación contractual. Este supuesto se entenderá sin perjuicio del art. 10 de la Directiva 97/7/CE y de las Directivas 95/46/CE (1) y 2002/58/CE».

Podríamos tomar el ejemplo de Doubleclick (adquirida por Google), cuya actividad consiste en administrar los espacios publicitarios de numerosas empresas activas en internet. Si Doubleclick envía de manera repetida *banners* publicitarios a los internautas, podría quedar sometida al anexo 1 de la directiva. En efecto, esta práctica podría formar parte de la lista negra promulgada por la directiva y prohibida bajo toda circunstancia.

3.1.2. Prohibición de las prácticas comerciales agresivas

§ 32. El art. 8 de la Directiva establece que «Se considerará agresiva toda práctica comercial que, en su contexto fáctico, teniendo en cuenta todas sus características y circunstancias, *merme o pueda mermar de forma importante, mediante el acoso, la coacción, incluido el uso de la fuerza, o la influencia indebida, la libertad de elección o conducta del consumidor medio*[81] con respecto al producto y, por consiguiente, le haga o pueda hacerle tomar una decisión sobre una transacción que de otra forma no hubiera tomado».

La pregunta es la siguiente: ¿una práctica comercial influencia un consumidor hasta el punto de quedar imposibilitado para tomar una decisión con conocimiento de causa?

(79) Podríamos imaginar que el ordenador personal pueda considerarse como el domicilio virtual del consumidor.

(80) El art. 2 a) de la Directiva da el definición de consumidor.

(81) El criterio de evaluación tomado por la Directiva es el *consumidor medio*, «que según la interpretación que ha hecho de este concepto el Tribunal de Justicia, está normalmente informado y es razonablemente atento y perspicaz, teniendo en cuenta los factores sociales, culturales y lingüísticos» (Considerando núm. 18 de la Directiva).

La Directiva proporciona algunos indicios para determinar la naturaleza leal de una práctica. El art. 9 contempla el uso del acoso, de la coacción o de una influencia injustificada y pone especialmente el acento sobre «a) el momento y el lugar en que se produce, su naturaleza o su persistencia». El Considerando n.º 16 insiste en que el art. 8 cubre «aquellas prácticas que mermen de forma significativa la libertad de elección del consumidor».

En el contexto del marketing, se detectan ciertas prácticas comerciales cuya naturaleza y persistencia podrían ordenarlas en el marco de la hipótesis a) del art. 9 y, por lo tanto, en la categoría de las prácticas agresivas. Por ejemplo, si los comerciantes recuerdan a sus clientes, cada vez que acuden a unos almacenes, que sería una buena idea comprar tal o cual camisa ya que han adquirido tal o cual pantalón sin haber comprado la camisa, ¿no podría esta actitud constituir una práctica comercial agresiva desleal? Igualmente, es legítimo preguntarse si el uso, por parte de un profesional, de la pasión devoradora de un consumidor por los videojuegos para influir sobre sus decisiones de compra en este campo, no se corresponde con la hipótesis c) del art. 9. Se podría añadir igualmente que la actividad desempeñada por Doubleclick[82], si no formara parte de la lista negra de las prácticas comerciales que se consideran desleales en cualquier circunstancia promulgadas por la directiva, podría aproximarse quizás al acoso en el sentido del art. 9.

§ 33. Además, la Directiva define «la influencia indebida» (art. 6 j) como la «utilización de una posición de poder en relación con el consumidor para ejercer presión, incluso sin usar fuerza física ni amenazar con su uso, de una forma que limite de manera significativa la capacidad del consumidor de tomar una decisión con el debido conocimiento de causa».

En el contexto del marketing, el comerciante corre el riesgo de explotar su posición dominante con respecto a los consumidores al ofrecerles determinado tipo de productos y no otros. Si esto les afecta de manera significativa, la práctica comercial caerá en el campo de aplicación del artículo. La cuestión está en saber si el comportamiento del comerciante limita significativamente la aptitud del consumidor para tomar una decisión con el debido conocimiento de causa. La frontera no es tan evidente pues

(82) *Cf. supra* n. 31.

el objetivo de las acciones de marketing consiste justamente en conducir a los consumidores hacia un tipo de producto determinado y no otro.

3.1.3. Prohibición general de prácticas comerciales desleales

§ 34. El art. 5 prohíbe de manera general las prácticas comerciales desleales. En efecto, podrían surgir nuevas prácticas que, sin ser engañosas ni agresivas, fueran desleales de todos modos. Dispone que:

> «1. Se prohibirán las prácticas comerciales desleales. 2. Una práctica comercial será desleal si:
>
> a) es contraria a los requisitos de la diligencia profesional, y
>
> b) distorsiona o puede distorsionar de manera sustancial, con respecto al producto de que se trate, el comportamiento económico del consumidor medio al que afecta o al que se dirige la práctica, o del miembro medio del grupo, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores».

El artículo define un «*standard* de comportamiento»[83]. Las dos condiciones exigidas son acumulativas. La primera condición es «objetiva»[84]. De conformidad con la definición que el art. 2 h) da a la «diligencia profesional», el profesional[85] no solo debe adoptar un comportamiento respetuoso con las buenas costumbres, sino que debe ser igualmente competente y concienzudo. El Juez deberá averiguar si «existe alguna norma equivalente a un comportamiento de referencia, como el de un buen padre de familia»[86]. Entonces la noción de «diligencia profesional» se aproximaría a la noción de culpa[87]. Para ser sancionado, el comerciante deberá cometer una falta que provoque un daño al consumidor, con un nexo de

(83) De Cordt, Y., Delforge, C., Leonard, Th. y Poullet, Y., *Manuel de Droit commercial*, Anthémis, Académie Universitaire Louvain, 2009, núm. 890, págs. 499.
(84) De Cordt, Y., Delforge, C., Leonard, Th. y Poullet, Y., *Manuel de Droit commercial*, *op. cit*, núm. 890, págs. 499.
(85) El art. 2 b) de la Directiva proporciona la definición de profesional.
(86) Ferrant, I., *Les pratiques du commerce (depuis les modifications législatives de 2007)*, Kluwer, Practique du droit, Tomo 34, 2008, núm. 103, pág. 51.
(87) De Brouwer, L., «La directive 2005/29/CE du 11 mai 2005 relative aux pratiques commerciales déloyales», *RDC* 2005/7, sept. 2005, pág. 793 y ss., esp. pág. 795.

causalidad entre estos dos elementos. El daño puede ser efectivo o simplemente potencial. Solo el interés económico es tomado en cuenta.

En relación con la segunda condición, «subjetiva»[88], que establece el art. 5.2, debe precisarse ante todo que solo se requiere la posibilidad de una alteración sustancial del comportamiento económico. Para que el art. 5 sea aplicable basta con que esta alteración sea potencial, no necesariamente efectiva. Luego, como preconiza el art. 2 e), está en juego la alteración sustancial del comportamiento económico cuando una práctica comercial amenaza considerablemente la aptitud del consumidor para tomar una decisión con pleno conocimiento de causa. La influencia de la práctica comercial sobre el comportamiento del consumidor debe ser pues determinante.

En este caso, las posibilidades que ofrece el marketing *one-to-one* son tan infinitas que deben ser inquietantes. Los riesgos consiguientes no son desdeñables. La explotación abusiva de las características psicológicas de un individuo podría caer bajo la aplicación del art. 5.

§ 35. Los arts. 5 y 2 e) están formulados en términos generales para poderse aplicar a toda práctica comercial desleal, aunque no sea engañosa ni agresiva. Sin embargo otras prácticas comerciales que se contentarían con influenciar el comportamiento de compra del consumidor pero sin mermar su aptitud para tomar una decisión con conocimiento de causa no caerían en el ámbito de la Directiva[89].

§ 36. El reto está en distinguir entre las prácticas comerciales que afectan legítimamente la percepción de los productos por los consumidores y los influencian sin amenazar su aptitud para tomar de decisiones informadas, y las prácticas comerciales que afectan considerablemente su aptitud para tomar tales decisiones. La frontera no es evidente. Y lo que es más, no parece inmutable. Algunas prácticas de marketing que, actualmente, se considera que afectan considerablemente la aptitud de los consumidores para tomar decisiones informadas, podrían, en un futuro más o menos cercano, devenir legítimas al ser aceptadas como una nueva norma. Cabe esperar

(88) De Cordt, Y., Delforge, C., Leonard, Th. y Poullet, Y., *Manuel de Droit commercial*, *op. cit.*, núm. 890, pág. 499.
(89) *Cfr.* el Considerando núm. 6.

que, entonces, los consumidores hayan aprendido, por su lado, a apartarse de su influencia...

3.2. *La violación de la legislación de protección de datos personales como práctica comercial desleal*

§ 37. ¿Podría ocurrir que, en el marco de nuestro contexto de marketing, una infracción de la legislación de protección de datos personales constituyera una práctica comercial desleal en el sentido de la Directiva 2005/29? En suma, ¿el hecho de no respetar las reglas relativas a la protección de datos personales podría ser una práctica comercial agresiva o desleal en un sentido más amplio? En otras palabras, ¿la violación de la legislación sobre la vida privada podría utilizarse en los procedimientos entablados por los consumidores contra los comerciantes? Ocurre que la legislación sobre datos personales ya se ha invocado en procedimientos entre empresas en situación de competencia para denunciar prácticas contrarias a los buenos usos del comercio (1). Según nuestros conocimientos, el recurso a esta legislación en los litigios entre consumidores y empresas para declarar una práctica comercial desleal no es frecuente de momento pero es, sin embargo, eficaz (2).

3.2.1. En los litigios entre empresas

§ 38. Las empresas en situación de competencia han invocado a menudo la legislación sobre datos personales para solicitar al Juez que declare un acto contrario a los buenos usos del comercio. La violación de tal disposición —por ejemplo, la cesión de datos de carácter personal sin el consentimiento de las personas afectadas, un tratamiento de datos incompatible con los objetivos originales...— conllevaría una competencia ilegítima en el mundo de los negocios. Así lo han decidido varias jurisdicciones. En el marco de una acción en cesación, los Jueces del Tribunal de apelación de Anvers[90] condenaron un banco por haber utili-

(90) CA Anvers, 3 de mayo de 1999, *AJT* 1999/2000, pág. 437, nota De Vos, C., Chronique de jurisprudence, «Vie privée» por Poullet, Y., *Les dossiers du Journal des Tribunaux*, Larcier, 2003, esp. núm. 151. Véase asimismo el asunto *FEBIAC*, Comm. Bruxelles (*prés.*), 12 de julio de 1996, *DA/OR* 1996, *liv.* 39, pág. 73; nota Ballon, G., *DCCR* 1996, pág. 351; nota Domont-Naert, F., RW, 1996/1997, pág. 855; nota Meeusen, J., Chronique de jurisprudence, «Vie privée» por Poullet, Y., *Les dossiers du Journal des Tribunaux*, Larcier, 2003, esp. núm. 153. Y el asunto KBC, Comm. Gand., 23 de abril de 1997, *TGR* 1997, pág. 174; Chronique de jurisprudence, «Vie privée» por Poullet, Y., *Les dossiers du Journal des Tribunaux*, Larcier, 2003, esp. núm. 152.

zado datos de su clientela, comunicados en el marco de órdenes de pago, para hacer publicidad de productos de seguro. La Corte ha cuestionado la legitimidad del tratamiento operado por el banco porque la utilización «marketing» por el banquero de datos comunicados para hacer una transferencia, excedía las previsiones razonables del cliente del banco. Solo el consentimiento de la persona afectada puede entonces ser la causa legítima de la utilización con fines de marketing, por el banco, de los datos relativos a la realización de una transferencia. Recientemente, el Tribunal de apelación de Bruselas ha estimado que la utilización por un banco de los datos personales registrados en ocasión de las órdenes de pago dadas por sus clientes, en un conflicto con sus agentes, constituye una violación de los buenos usos en materia comercial[91]. El incumplimiento de una disposición legal —en este caso la legislación de protección de datos de carácter personal— en el ejercicio del comercio, puede representar una violación de los buenos usos en materia comercial. Incluso ha ocurrido que el Juez haya comprobado incidentalmente, en el contexto de una acción de cesación, si el responsable ha cumplido su obligación de declaración de los tratamientos automatizados[92].

3.2.2. En los litigios entre consumidores y empresas

§ 39. Los consumidores podrían emprender la misma iniciativa que se ha producido ya entre sociedades. En la medida en que una infracción de la legislación de protección de los datos de carácter personal respondería a la definición de una práctica comercial desleal en el sentido de la Directiva 2005/29, no existe, *a priori*, ningún obstáculo para que el consumidor invoque esta infracción en el marco de una acción de cesa-

(91) CA Bruxelles, 15 de febrero de 2005, *Pratiques du Commerce et Concurrence – Annuaire 2005*, De Bauw, H. (ed.), Kluwer, 2006, pág. 495 y ss.

(92) Aff. Belgacom, Comm. Bruxelles (*prés*), 19 de junio de 1995, *JT* 1995, pág. 188; Chronique de jurisprudence, «Vie privée» por Poullet, Y., *Les dossiers du Journal des Tribunaux*, Larcier, 2003, esp. núm. 165.

ción contra un comerciante[93]. Es lo que ocurrió en un caso que opuso la asociación de consumidores Test-Achats al banco Fortis. La asociación de consumidores reprochaba a la sociedad que concluyera contratos de hospitalización individual con sus clientes utilizando documentos contractuales que contenían muchas infracciones a la Ley de la vida privada. Por un lado, el responsable del tratamiento debe tomar todas las medidas técnicas y organizativas para garantizar la confidencialidad de los datos tratados. Por lo tanto, el hecho de fusionar el cuestionario médico con la propuesta de seguro sin implantar ninguna medida de protección de la confidencialidad de los datos médicos, infringe la Ley. Por otra parte, el hecho de que se encontrara el cuestionario médico en manos del asegurador, viola la regla según la cual los datos personales médicos deben tratarse bajo la responsabilidad de un profesional de salud. Estas infracciones de la legislación de protección de datos personales constituyen prácticas contrarias a los buenos usos en materia comercial. Estos son los términos en que se pronunció el Tribunal de apelación de Bruselas, el 16 de junio de 2003: «la práctica que consiste en fusionar en un solo documento la propuesta de seguro y el cuestionario médico es contraria a los buenos usos en materia comercial»[94].

§ 40. Así pues, se revela completamente posible que Test-Achats entablara otras acciones de cesación sobre la base de una práctica comercial desleal constituida por una infracción de la legislación sobre datos personales, en muchos otros ámbitos y especialmente el marketing *one-to-one*. La violación de estas disposiciones deberá entrar en el campo de aplicación del art. 8 de la Directiva 2005/29, referente a las prácticas comerciales agresivas[95], o bien en la definición del art. 5 dedicado a las prácticas comerciales desleales que no serían ni engañosas ni agresivas.

(93) Comp. en Estados Unidos, la *Federal Trade Commission* que hace aplicar la Ley sobre las prácticas comerciales desleales y engañosas y que tiene el poder de entablar acciones contra las empresas que se libran a tales prácticas (incluidas las que no respetan su *privacy policy*). Sobre el tema, véase King, N. J., «When mobile phones are RFID-equiped-Finding EU-US solutions to protect consumer privacy and facilitate mobile commerce», *Michigan Telecommunications and Technology Law Review*, vol. 15, N.° 1, Otoño de 2008, esp. págs. 157, 166, 191 y 195.

(94) Comm. Bruxelles (cess.), 16 de junio de 2003, *DCCR* núm. 163, 2004, pág. 104.

(95) O engañosas.

4. Conclusiones

§ 41. Las conclusiones de tal análisis serían múltiples. Las limitaremos a dos puntos esenciales. El primero se refiere al interés, puesto de relieve en las reflexiones del capítulo 2, de una aproximación que los autores americanos califican de *Consumer Privacy*, es decir de una aproximación que combina la protección de la vida privada y la protección de los consumidores. El segundo es más fundamental. Enseña que las posibilidades que descubren la utilización de las técnicas de *profiling* y la inteligencia ambiental —lo que se ha dado en llamar el *internet of Things*[96]—, obligan a reabrir los debates fundamentales que subyacen en la consagración de la «vida privada» y dan a este concepto un alcance que va mucho más allá de las legislaciones de protección de datos.

4.1. El interés de la aproximación «Consumer Privacy»

§ 42. Nuestro trabajo aboga por esta aproximación. Más allá de los temas relacionados con los derechos humanos, el desarrollo de las tecnologías de la información y sus aplicaciones presentan implicaciones económicas importantes para la defensa de los consumidores. La economía de internet reposa ampliamente sobre recursos publicitarios y las tecnologías que la animan confieren a quienes desean maximizar el interés de la publicidad, los medios apropiados para hacerlo. El marketing *one-to-one* se encuentra en plena expansión y la aparición de sociedades especializadas en técnicas de prospección y de empresas —como las plataformas del web 2.0 o como Google— en relación directa con los individuos que «consumen» sus servicios altamente personalizados hacen temer una explotación cada vez más aguda de la expresión de las elecciones de los consumidores o de datos de carácter altamente personal que estos confían a la red (lista de amigos, hobbies, fotos de vacaciones, etc.). En definitiva, la protección de los consumidores y de la vida privada encuentran una causa común, alentada por las disposiciones legales: utilización de las disposiciones en materia de prácticas comerciales desleales o agresivas, posibilidad de acciones colectivas y, más allá, interés de un acercamiento de las autoridades de protección de

(96) Sobre este tema, léase Rouvroy, A., «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence», *Studies in Ethics, Law, and Technology*, Berkeley Electronic Press, 2008.

los datos, de las asociaciones de libertades civiles y de las asociaciones de protección de los consumidores. El interés de esta aproximación común se confirma por el análisis de la acción notable del *Federal Trade Commission* americana[97] en materia de *Privacy*. A pesar de la ausencia de legislación en materia de protección de datos, esta jurisdicción administrativa especializada en materia de protección de los consumidores ha podido desarrollar una reflexión y acciones importantes en los campos que ahora nos ocupan, ya se trate del uso para fines comerciales de los RFID[98], ya de las técnicas de *profiling*[99]. Esta acción se ha podido desarrollar sobre base de la Ley americana relativa a las prácticas desleales, en particular sobre la base del *False and Deceiptive Statement Act* y debería inspirar nuestras propias autoridades públicas de protección de los consumidores.

4.2. *Más allá de la protección de datos de carácter personal, un debate fundamental para nuestras libertades*

§ 43. La *privacy* como protección de la «autodeterminación informativa» es un concepto más amplio que la protección de datos y conduce a debates más fundamentales sobre el conjunto de nuestras libertades, en la

(97) Ver el sitio remarcable de la FTC http://www.ftc.gov/. El 22 de julio de este año, la FTC informaba ante la Comisión senatorial americana «*Commerce, Science and transportation*», en materia de «*Advertising trends and Consumer Protection*».

(98) Sobre esta acción en materia de RFID y la importancia en este contexto de la asociación CASPIAN de protección de los consumidores, asociación especializada en la temática de los RFID, léase King, N., «Direct Marketing, Mobile Phones and Consumer Privacy Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices», *Federal Communications Law Journal*, marzo de 2008, 2, Vol. 60, pág. 229 y ss.

(99) Léase en particular la memoria sobre «Online Behavioral Advertising Moving the Discussion Forward to Possible Selfregulatory Princples», disponible en el sitio de la FTC: http://www.ftc.gov.bcp/ y los debates sobre el tema mantenidos los días 1 y 2 de noviembre de 2007: «Behavioral Advertising: Tracking, Targeting and Technology». Véase asimismo World Privacy Forum, *The Network Advertising Initiative: Falling at Consumer Protection and Selfregulation*, publicado el 2 de noviembre de 2007 sobre el sitio: http://www.worldprivacyforum.org. Muy recientemente (13 de enero de 2009) el «*Center for Digital Democracy*», centro especializado en derechos del hombre, ha dirigido una queja ante la FTC (disponible en línea). Esta queja contiene una memoria que detalla la estrategia de diferentes sociedades americanas en este campo y la amplitud de los riesgos vinculados a estas prácticas, en particular por el uso de datos relacionados con la tenencia de teléfonos móviles.

medida que es una condición para todas ellas[100]. Los problemas relacionados con el desarrollo de estas nuevas tecnologías inteligentes muestran que el *privacy* no es solo una lucha para proteger la intimidad o de la pérdida de control de nuestros datos personales. Tiene un alcance mucho mayor. El debate sobre la *privacy* cambia de naturaleza. Más allá de la protección que ofrece la legislación sobre datos de carácter personal —y de que sea aplicable o no[101]— es preciso subrayar que varios derechos fundamentales parecen amenazados. Recordemos, antes de enumerarlos, el sacro santo principio afirmado por el art. 1 de la Carta de los derechos fundamentales de la Unión Europea según que la dignidad humana es inviolable y debe ser respetada y protegida. La dignidad humana debe guiar todas nuestras reflexiones en la materia. Esta directriz es fundamental en nuestras tradiciones y culturas jurídicas occidentales: responde al imperativo ético kantiano según cual el modo del que concebimos y vivimos nuestras relaciones con los demás debe inspirarse en el hecho de que estos no son nunca un medio para alcanzar un fin, sino, siempre, un fin en sí mismo. Este principio excluye una visión puramente utilitarista de nuestras relaciones con los demás —consumidores de productos o servicios de grandes superficies en el marco de nuestro escenario—. Entre los derechos fundamentales arañados por las tecnologías inteligentes, cabe citar ante todo el derecho al respeto de la integridad física y mental[102]. Si las acciones de marketing personalizado ejercen una influencia demasiado importante sobre las elecciones de los consumidores, podría sostenerse que se está amenazando su integridad mental. Este impacto sería efectivo en la hipótesis de una manipulación psicológica excesiva hasta el punto de afectar el comportamiento de los consumidores. Luego, la libertad de pensamiento, de conciencia y de reli-

(100) Sobre la *privacy* como libertad «fundamental», léase Burkert, H., «Dualities of Privacy – An Introduction to "Personal Data Protection and Fundamental Rights"», *in Défis du droit à la protection de la vie privée*, Pérez, M. V., Palazzi, A. (eds.), Cahier du Crid, 2008, págs. 13 y ss. Véanse asimismo nuestras reflexiones en Rouvroy, A. y Poullet, Y., «The right to informational self-determination and the value of self-development – Reassessing the importance of privacy for democracy», en *Reinventing Data Protection*, Colloque tenu à Bruxelles, Nov. 2007, Springer Verlag, Dordrecht, 2009, págs. 50 y 51.

(101) *Cfr.* nuestras reflexiones *supra* núm. 8 y ss.

(102) *Cfr.* el art. 3 de la Carta de los Derechos Fundamentales de la Unión Europea de 18 de diciembre de 2000.

gión[103] —que pretende asegurar la diversidad cultural, religiosa y filosófica indispensable en nuestras sociedades democráticas[104]— parece en peligro en el sentido que las aplicaciones de las tecnologías de la información pueden conducir a una normalización del pensamiento[105]. Además, el recurso a la técnica del *dynamic pricing*, que provoca que el precio solicitado a los consumidores para un determinado producto no sea el mismo siguiendo criterios poco razonables[106], crea el riesgo de provocar discriminaciones[107] y hace peligrar así el derecho de gozar de estas libertades sin discriminación[108]. En fin, la libertad de movimiento[109], que implica que nos podamos desplazar sin ser seguidos constantemente o «trazado», está igualmente amenazada[110].

§ 44. Concluyamos. Es evidente que las tecnologías de la información proporcionan una ocasión de liberarse, de descubrir mundos nuevos, de dejar atrás coacciones que tejen su círculo existencial, de expresarse y de

(103) Art. 18 de la DUDH (10 dic. 1948); art. 9 CEDH (1950); art. 10 de la Carta Europea de los Derechos Fundamentales (2000).

(104) «*The pluralism indivisible from a democratic society depends on it*»: CAMMILLERI-SUBRENAT, A. y LEVALLOIS-BARTH, C., *Sensitive Data Protection in the European Union*, *op. cit.*, esp. pág. 102.

(105) *Cfr.* la decision del Tribunal Constitutional alemán. Véase asimismo VAN DER HOF, S. y PRINS, C., «Personalisation and its influence in identities, behaviour and social values», en *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. HILDEBRANDT y S. GUTWIRTH (ed.), *op. cit.*, esp. pág. 121.

(106) Véase *supra*.

(107) VAN DER HOF, S. y PRINS, C., «Personalisation and its influence in identities, behaviour and social values», en *Profiling the European Citizen, Cross-Disciplinary Perspectives*, M. HILDEBRANDT y S. GUTWIRTH (ed.), *op. cit.*, esp. pág. 121. Los mismos autores, sin embargo, matizan con razón sus afirmaciones: «*Personalisation is an effective tool to achieve an efficient market*».

(108) Art. 2 de la DUDH; art. 14 de la CEDH; art. 21 de la Carta Europea.

(109) Art. 2 del Protocolo adicional núm. 4 de la Convención del Consejo de Europa; art. 45 de la Carta de los Derechos Fundamentales de la Union Europea. Como pone de relieve la Opinión 4/2004 del Grupo de trabajo del art. 29, la libertad de movimiento debe entenderse en sentido amplio: «*Freedom of movement (...) means (...) also that one must be free to move without inevitably leaving continuous and/or frequent traces of one's movements for the benefit of systems enabling permanent optical observation and grassing out. Being seen without seeing may indeed constrain the person in their movements and trajectories*».

(110) Véase KING, N., «Direct Marketing, Mobile Phones and Consumer Privacy Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices», art. cit.

comunicarse con quien se desee. Es innegable que aportan ventajas tanto sobre el plano económico (compra a distancia, economía de desplazamientos) como sobre el plano de la seguridad (sistema de videovigilancia).

Pero estas mismas tecnologías representan una amenaza, tanto más grande para nuestras libertades cuanto las ventajas que avanzábamos nos conducen a multiplicar sus riesgos: aceptar no solo a ser seguidos, a vernos reducidos a un número, a sufrir mensajes que llegan a nuestros buzones a todas horas, sobre nuestras pantallas e incluso en nuestros cuerpos sino, además, a jugar el juego de la mercantilización de la información personal, exhibiéndonos en la red a través de las redes sociales y otros. En este punto en particular, un elemento esencial del derecho a la protección de la vida privada es la defensa de la persona humana, de su desarrollo y de su dignidad como valores absolutas; y eso pasa por devolver las lógicas absolutas de la seguridad y la eficacia económica a su dimensión totalmente relativa.

Nuestra reflexión acaba o, más bien, se abre; reclama un debate amplio, si es posible europeo, otorgando a todas las categorías de intereses, las empresas presentes en la web, los proveedores de equipos terminales, los *designers* de sistemas de información, los consumidores, las asociaciones de libertades, las autoridades de protección de datos, los organismos oficiales de protección de los consumidores, la posibilidad de poder expresarse sobre estas nuevas aplicaciones de las tecnologías, su impacto tanto en materia de protección de los consumidores como de protección de las libertades. No se trata de despreciar el provecho que estas tecnologías representan para los ciudadanos, sino de velar por una mejor educación del público, de recordar los imperativos reglamentarios en la materia y a valorar y sobre todo a buscar colectivamente, incluyendo a la propia tecnología, las soluciones que se impongan.